Appl. No. 09/706,728
Reply to Office Action of May 7, 2004

Docket No.: T2147-906625

AMENDMENT TO THE CLAIMS:

This listing of claims will replace all prior versions of claims in the application.

Listing of Claims:

1-14.   (Cancelled)

15.   (Currently Amended) An encryption circuit ~~(1)~~ for simultaneously processing various encryption algorithms, the <u>encryption</u> circuit adapted to be coupled with a host computer system ~~(HS), characterized in that the circuit comprises~~ <u>comprising</u>:

[[-]] an input/output module ~~(2), for handling~~ <u>that handles</u> data exchanges between the host <u>computer</u> system ~~(HS)~~ and the <u>encryption</u> circuit ~~(1)~~ via a dedicated bus ~~(PCI)~~,

[[-]] an encryption module ~~(3)~~ coupled with the input/output module, ~~(2)~~ said encryption module controlling encryption and decryption operations, as well as storage of all sensitive information ~~(1)~~ of the <u>encryption</u> circuit; and

[[-]] isolation means ~~(4)~~ between the input/output module ~~(2)~~ and the encryption module ~~(3), for making~~ <u>the isolation means makes</u> the sensitive information stored in the encryption module ~~(3)~~ inaccessible to the host <u>computer</u> system ~~(HS)~~ and ~~for ensuring the~~ <u>ensures</u> parallelism of the operations performed by the input/output module ~~(2)~~ and the encryption module ~~(3)~~.

16.   (Currently Amended) An encryption circuit according to claim 15, ~~characterized in that~~ <u>wherein</u> the isolation means ~~(4) of the circuit (1)~~ comprises a ~~double~~<u>dual</u>-port memory ~~(4)~~.

2

17.   (Currently Amended) An encryption circuit according to claim 15, wherein ~~this~~ the isolation means (4) comprises a ~~double~~ dual-port memory coupled between the input/output module (2) and the encryption module (3), the dual-port memory (4) being coupled to a first bus and adapted to simultaneously handle the exchange of data, commands and statuses between the input/output and encryption modules (2 and 3), and isolation between the ~~two modules (2 and 3)~~ input/output and encryption modules.

18.   (Currently Amended) An encryption circuit is set forth in claim 15, ~~characterized in that~~ wherein the encryption module (3) comprises:

[[-]] a first encryption sub-module (3₁), dedicated to the processing of symmetric encryption algorithms, and being coupled with ~~the~~ a first bus of the dual-port memory (4);

[[-]] a second encryption sub-module (3₂), dedicated to the processing of asymmetric encryption algorithms (40) and being coupled with the first bus of the dual-port memory (4) and including a separate internal second bus isolated from the first bus of the dual-port memory (4); and

[[-]] a CMOS memory, (11) coupled with the dual-port memory (4) via the first bus of the dual-port memory, containing the encryption keys.

19.   (Currently Amended) An encryption circuit as set forth in claim 16, ~~characterized in that~~ wherein the encryption ~~modules (3)~~ module comprises:

[[-]] a first encryption sub-module (3₁), dedicated to the processing of symmetric encryption algorithms, and being coupled with ~~the~~ a first bus of the dual-port memory (4);

[[-]] a second encryption sub-module (3₂), dedicated to the processing of asymmetric encryption algorithms (40) and being coupled with the first bus of the dual-port memory (4)

3

and including a separate internal second bus isolated from the first bus of the dual-port

memory (4); and

[[-]] a CMOS memory, (11) coupled with the dual-port memory (4) via the first bus of

the dual-port memory, containing the encryption keys.

20.   (Currently Amended) An encryption circuit as set forth in claim 17,

~~characterized in that~~ wherein the encryption module (3) comprises:

[[-]] a first encryption sub-module (3₁), dedicated to the processing of symmetric

encryption algorithms, and being coupled with the first bus of the dual port memory (4);

[[-]] a second encryption sub-module (3₂), dedicated to the processing of asymmetric

encryption algorithms (40) and being coupled with the first bus of the dual-port memory (4)

and including a separate internal second bus isolated from the first bus of the dual-port

memory (4); and

[[-]] a CMOS memory, (11) coupled with the dual-port memory (4) via the first bus of

the dual-port memory, containing the encryption keys.

21.   (Currently Amended) ~~an~~ An encryption circuit according to claim 18,

~~characterized in that~~ wherein the first encryption sub-module (3₁) comprises an encryption

component (9) coupled with the dual-port memory (4) via the first bus of the memory (4),

comprising various encryption automata, respectively dedicated to the processing of

symmetric encryption algorithms, and in that the second encryption sub-module (3₂)

comprises at least two encryption processors (10₁ and 10₂), respectively dedicated ~~tot he~~ to

the processing of asymmetric encryption algorithms, coupled with the encryption module (9)

via the internal second bus of the second sub-module (3₂) and a bus isolator (14) for isolating

that isolates the second bus from the first bus of the dual-port memory.

22.   (Currently Amended) An encryption circuit according to claim 21,

characterized in that wherein the encryption processors (10₁ and 10₂) of the encryption

module (30 are of the CIP type configuration.

23.   (Currently Amended) An encryption circuit according to claim 21,

characterized in that wherein one (10₁) of the two encryption processors (10₁ and 10₂) is of

the CIP type, and in that the other (10₂) of the two encryption processors is of the ACE type

configuration.

24.   (Currently Amended) An encryption circuit according to claim 21,

characterized in that wherein one of the two encryption processor (10₂) is of the ACE type

configuration comprising a field programmable gate array (FPGA).

25.   (Currently Amended) An encryption circuit according to claim 24,

characterized in that wherein the encryption component (9) is of the SCE type configuration.

26.   (Currently Amended) An encryption circuit according to claim 25,

characterized in that wherein the encryption component (9) comprises a field programmable

array (FPGA).

Appl. No. 09/706,728
Reply to Office Action of May 7, 2004

Docket No.: T2147-906625

27.   (Currently Amended) An encryption circuit according to claim 26, ~~characterized in that~~ <u>wherein</u> the second encryption sub-module ~~(3₂)~~ comprises a flash memory PROM ~~(12)~~ and an SRAM memory ~~(13)~~ coupled with the second internal bus of the sub-module ~~(3₂)~~.

28.   (Currently Amended) An encryption circuit according to claim 21, further comprising a CMOS memory ~~(11)~~ containing security keys and security mechanisms ~~(15)~~ adapted to trigger a reset mechanism of the CMOS memory ~~(11)~~ in case of an alarm.

29.   (Currently Amended) ~~an~~ <u>An</u> encryption circuit according to claim 15, ~~characterized in that~~ <u>wherein</u> the input/output module ~~(2)~~ comprises:

[[-]] a microcontroller ~~(6)~~ having an input/output processor ~~(6₁)~~ and a PCI interface ~~(6₂)~~ integrating DMA channels responsible for executing the data transfers between the host <u>computer</u> system ~~(HS)~~ and the circuit ~~(1)~~;

[[-]] a flash memory ~~(7)~~ containing the code of the input/output processor ~~(6₁)~~ and a PCI interface ~~(6₂)~~ integrating DMA channels responsible for executing the data transfers between the host <u>computer</u> system ~~(HS)~~ and the circuit ~~(1)~~;

[[-]] a flash memory ~~(7)~~ containing the code of the input/output processor ~~(6₁)~~; and

[[-]] an SRAM memory ~~(8)~~ that receives a copy of the contents of the flash memory ~~(7)~~ upon startup of the input/output processor ~~(6₁)~~.

30.   (Currently Amended) An encryption circuit according to claim 15, comprising a serial link ~~(SL)~~ connected to input basic keys through a secure path independent of the dedicated PCI bus, said link adapted to be controlled by the encryption module ~~(3)~~.

Appl. No. 09/706,728
Reply to Office Action of May 7, 2004

Docket No.: T2147-906625

31.   (Currently Amended) An encryption circuit according to claim 30,

~~characterized in that~~ <u>wherein</u> the serial link (SL) allows downloading of proprietary

algorithms into the first encryption sub-module ~~(3₁)~~.

32.   (Original) An encryption circuit as set forth in claim 15, further including a

card supporting the circuit.

33.   (Original) An encryption circuit as set forth in claim 18, further including a

card supporting the circuit.

34.   (Original) An encryption circuit as set forth in claim 21, further including a

card supporting the circuit